

FILED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT GREENEVILLE

JAN 31 2023

Clerk, U. S. District Court
Eastern District of Tennessee
At Greeneville

IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT
656 MOUNTAIN VIEW ROAD, LOT 27
BLUFF CITY, TN 37618

2:23-MJ-16_____

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Peter Evans, a Special Agent with Homeland Security Investigations in Johnson City, Tennessee, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI) and have been so employed since July 2017. I am currently assigned to the HSI Johnson City office where I investigate a wide variety of criminal violations. While employed at HSI I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography. I have completed multiple Law Enforcement Training Academies including HSI Special Agent Training and the Criminal Investigator Training Program at the Federal Law Enforcement Training Center. I have received training in child pornography and child exploitation investigations and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256). I have participated in numerous investigations into offenses involving child pornography and child exploitation. Through my work in these investigations, as well as my discussions with other experienced agents, I have experience in examining evidence and estimating the approximate ages of

individuals depicted in photographs and videos. I have a bachelor's degree in Criminal Justice, and I have been a sworn federal law enforcement officer since 2011.

2. This affidavit is made in support of an application for a warrant to search the premises of 656 Mountain View Road, Lot 27, Bluff City, TN 37618 (the "**SUBJECT PREMISES**"), more fully described in Attachment A, and to seize evidence, more fully described in Attachment B, of violations of 18 U.S.C. Section 2252(a)(2) and 18 U.S.C. Section 2252(a)(4)(B). 18 U.S.C. Section 2252(a)(2) makes it a crime for any person to knowingly receive or distribute material that depicts minors engaged in sexually explicit conduct that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer. 18 U.S.C. Section 2252(a)(4)(B) makes it a crime for any person to knowingly possess any material that depicts minors engaged in sexually explicit conduct that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

3. The statements in this affidavit are based on my personal observations, training, experience, and information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for this warrant.

DEFINITIONS

4. The following definitions apply to this Affidavit and its Attachments:
- a. **Kik messenger** is a mobile messaging device application available on Android and Apple devices and advertises itself as "the best way to connect with friends, no matter where

you meet them. But it's also become so much more. As the only chat platform built especially for teens and as a clear leader in chatbots, Kik will become the central hub for everyday life for teens across the world as we grow." According to Kik's website they were "founded in 2009 by a small but passionate group of University of Waterloo students. At the time, chat between Blackberry (yes, Blackberry), Android and iPhone users wasn't possible, so we wanted to break down barriers and build a company that would allow users to chat with whoever, whenever."

b. National Center for Missing and Exploited Children (NCMEC) is a private, non-profit 501(c)(3) corporation whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC works with families, victims, private industry, law enforcement, and the public to assist with preventing child abductions, recovering missing children, and providing services to deter and combat child sexual exploitation. NCMEC receives cyber tips related to child exploitation and forwards them to the appropriate Internet Crimes Against Children (ICAC) Taskforce.

c. The ICAC is a national network of 61 coordinated task forces, representing over 5,400 federal, state, and local law enforcement, dedicated to investigating, prosecuting, and developing effective responses to internet crimes against children.

d. The term "child pornography" as used herein, means any visual depiction of sexually explicit conduct involving a minor.

e. The term "minor" is defined at 18 U.S.C. § 2256(1) as any person under the age of eighteen years.

f. The term "sexually explicit conduct" is defined at 18 U.S.C. § 2256(2)(A) as actual or simulated - (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or anal-oral, whether between person of the same or opposite sex; (ii) bestiality; (iii) masturbation;

(iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person.

g. The term “computer” is defined as set forth in 18 U.S.C. § 1030(e)(1).

h. The term “IP” (Internet Protocol) is defined as the primary protocol upon which the Internet is based. An IP allows a packet of information to travel through multiple networks (groups of linked computers) on the way to its ultimate destination.

i. The term “IP Address” is defined as a unique number assigned to every computer directly connected to the Internet (for example 172.191.142.150). Each computer connected to the Internet is assigned a unique IP address while it is connected. The IP address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP address is only assigned for the duration of that on-line session.

j. The term “ISP” (Internet Service Provider) is defined as a business that allows a user to dial into or link through its computers thereby allowing the user to connect to the Internet for a fee. ISPs generally provide only an Internet connection, an electronic mail address, and maybe Internet browsing software. A user can also connect to the Internet through a commercial online service such as America Online, Earthlink, or MSN. With this kind of connection, the user gets Internet access and the proprietary features offered by the online service, such as chat rooms and searchable databases.

k. The American Registry for Internet Numbers (ARIN) is a nonprofit, member-based organization that administers IP addresses in support of the operation and growth of the Internet. Information related to which ISP’s manages an IP address is publicly available from multiple websites on the internet.

1. The term “computer system and related peripherals, and computer media” as used in this affidavit refers to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

5. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet are critical components in the production, distribution, and collection of child pornography.

6. A child pornography image or video taken with a digital camera or cellular phone can be transferred directly to a computer, and then transferred from that computer to any other server or computer connected to the Internet via modem or wireless connection. Many devices not traditionally thought of as computers, such as video game consoles, smartphones, and digital media players, have the ability to store digital data, access the Internet, and send or receive digital data electronically.

7. The large storage capacity of current personal computers and external hard drives make them ideal repositories for child pornography. External hard drives with capacities of one or more terabytes are inexpensive and common. A terabyte is one thousand gigabytes. An inexpensive and portable flash drive can contain several gigabytes of data.

8. Child pornography collectors may use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Google, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

9. Communications made to or from a computer or other digital storage or communications device are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer, or by saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary "cache" folders. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and the contents of some of the files that were uploaded or downloaded.

10. Computer files or remnants of such files can be recovered years after they were viewed, downloaded, or deleted. Deleted files can often be recovered months or years later using readily available forensic tools. This is because a deleted file does not actually disappear; rather, it remains on the computer's hard drive until it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery"

file. Files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

ABOUT THE SEARCH AND SEIZURE OF COMPUTER SYSTEMS

11. When searching and seizing evidence from computers, agents commonly download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer-related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. The latter approach is more typical for the following two reasons:

a. The large storage capacity of modern digital storage devices assists in the concealment of criminal evidence, especially when the user camouflages digital files in the way they are named or stored. Sorting criminal evidence from innocuous data may thus take days or weeks, depending upon the volume of data stored, and is generally difficult to accomplish on-site. Also, some information on the computer may only make sense in the context of other information that must be analyzed with it. For example, an apparently meaningless series of letters and numbers may only be recognized as a password when described as such by another document, such as an email.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in particular

systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Because computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

12. To fully retrieve data from a computer system, a computer forensic analyst needs all magnetic storage devices as well as the central processing unit (“CPU”). In cases involving child pornography, where the evidence typically includes graphics files, the user’s monitor may be essential for a thorough and efficient search due to software and hardware configuration issues. Other elements of the computer, such as keyboards, mice, cables, and power cords, are necessary in order to ensure that the computer will continue to function in a laboratory environment. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

13. In case any data on the computer or other devices is encrypted, password-protected, or booby-trapped, a forensic analyst would require any documentation or notes describing password-protection or encryption software used on the computer or listing passwords and usernames.

SEARCH PROCEDURE

14. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel (which may include both federal and state law enforcement agents) executing the search warrant will employ the following procedure:

a. *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, “computer personnel”), if present, may be able to determine if digital devices can be searched on-site in a reasonable amount of time and without jeopardizing the health and safety of officers or residents. If practicable, computer personnel may have the ability to conduct a forensic preview of a device and try to preserve data on the device. Any device forensically previewed on-site will be seized if it contains any data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

b. *On-site imaging, if practicable.* If a digital device cannot be searched on-site as described above, the computer personnel, if present, will determine whether the device can be imaged on-site in a reasonable amount of time without jeopardizing the health and safety of officers, residents, or the ability to preserve the data and conduct such imaging if deemed practicable.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel (potentially including, but not necessarily limited to, computer personnel) will examine the digital device to determine if it contains any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B.

FACTS SUPPORTING PROBABLE CAUSE

15. On December 1, 2022, NCMEC received information from Kik Messenger that Kik user thom6058 had, uploaded/shared with another user or group of users, nine video files of child pornography. Kik provided information to include the following:

- a. Kik Subscriber Name: Thomas LLOYD
- b. Kik Subscriber Email Address: kthefrog562@gmail.com
- c. Kik Screen/Username: thom6058
- d. Kik User ID: thom6058_vck
- e. IP Address: 96.33.13.62 (Login) 11-11-2022 10:51:42 UTC

16. I viewed the cyber tip from NCMEC and confirmed that each of the nine video files contained child pornography. Each of the files had been uploaded between October 27-28, 2022, from IP address: 96.33.13.62. The following is an example of one of the files:

- a. File Name: 1faab48c-01bc-43f8-963b-498768796ba3.mp4
- b. Description: This file is a video approximately ten seconds long depicting a prepubescent female child being vaginally penetrated by an adult male's penis.

17. On January 18, 2023, Charter Communications provided subscriber information to include the following for the subscriber assigned 96.33.13.62 on 11/11/2022.

- a. SUBSCRIBER RECORD
 - i. Target Details 96.33.13.62, 55038, 11/11/2022 10:51:00 AM, GMT, 0
 - ii. Subscriber Name: THOMAS LLOYD
 - iii. Service Address: 656 MOUNTAIN VIEW RD, LOT 27, BLUFF CITY, TN 376183252

iv. Billing Address: 656 MOUNTAIN VIEW RD LOT 27, BLUFF CITY, TN
376183252

v. Username or Features: ROTCH97@GMAIL.COM

vi. Phone number: 4236769225

b. Advanced Subscriber Info

i. Account Number: 8353300080183031

ii. MAC: 80787120C50B

iii. Lease Log: Start Date: 04/01/2022 03:36 PM End Date: 01/12/2023 07:50
AM

18. The information from Charter Communications revealed that Thomas LLOYD has been assigned IP address 96.33.13.62 since April 1, 2022, through January 12, 2023. This time period encompasses all of the dates referenced in the cyber tip for when the child pornography was shared and when the user logged into his Kik account according to the cyber tip.

19. On January 18, 2023, I conducted record checks in a public records data base revealing that Thomas Tibbs LLOYD, date of birth 04/17/1977, social security number 226-15-0814, lived at 656 Mountain View Road, Lot 27, Bluff City, TN 37618, in Sullivan County. This data base also listed an older address from 2019 as 4573 Bluff City Hwy, Lot 10, Bluff City, TN 37618.

20. On January 18, 2023, I conducted record checks with the Tennessee Department of Safety revealing that Thomas Tibbs LLOYD, date of birth 04/17/1977, has a suspended TN driver's license #136076299 which listed his previous address of 4573 Bluff City Hwy, Lot 10, Bluff City, TN 37618.

21. On January 18, 2023, HSI SA Travis Carrier conducted surveillance at 656 Mountain View Road, Lot 27, Bluff City, TN 37618 and observed a Jeep SUV with license plate tag 133BDVR and a Ford SUV with no tag.
22. On January 24, 2023, I conducted record checks with the Tennessee Department of Safety revealing that the license plate tag 133BDVR was registered to Annette Shontel Rotch, who also had a suspended TN drivers license # 120171950. This license listed the same previous address mentioned above, 4573 Bluff City Hwy, Lot 10, Bluff City, TN 37618.
23. I conducted record checks in a public records data base revealing that an Annette Rotch currently lived at 656 Mountain View Road, Lot 27, Bluff City, TN 37618.

CHARACTERISTICS OF CHILD PORNOGRAPHY OFFENDERS

24. Based upon my knowledge, experience, and training in child pornography and online child exploitation investigations, and on the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:
 - a. People who distribute, transport, receive, or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, may receive sexual gratification, stimulation, and satisfaction from contact with children or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in images or videos, or in writings describing such activity.
 - b. People who distribute, transport, receive, or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, may collect sexually explicit or suggestive materials in a variety of analog or digital

media, including photographs, magazines, videos, books, drawings, videotapes, sometimes on reel-to-reel film, or on computer storage devices. These people use these materials for their own sexual gratification, to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to teach a child how to perform various sexual acts.

c. People who distribute, transport, receive or possess child pornography and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, often keep copies of child pornography material; that is, their child pornography collections, correspondence, mailing lists, and related books, whether in digital or other forms, in the privacy and security of their home, or at some other secure location. They prize this material and usually keep it for many years.

d. People who distribute, transport, receive, or possess child pornography and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, may correspond with or meet others interested in child pornography so that they can share information and materials. Oftentimes, this correspondence occurs via the Internet and chat-logs, e-mails and records of the correspondence are stored on the users' computers or digital storage media devices. Child pornography collectors often keep lists of names, usernames, e-mail addresses or other contact information for individuals with whom they have been in contact and who share the same interests.

e. People who distribute, transport, receive or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes commonly create online profiles or user accounts using fake names and images of other individuals or images not attributable to their true selves. These individuals do this in an attempt to conceal their true identities from law enforcement and/or to entice minors for sexual purposes.

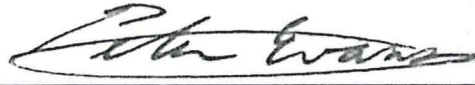
f. People who distribute, transport, receive or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes normally use multiple digital storage media devices, computers and external storage media in their possession to receive, possess and distribute child pornography and/or other material related to the sexual exploitation of children. Individuals who use applications on their smartphones or tablet computers to discuss the sexual exploitation of children or trade child pornography commonly also do so on their personal computers or laptops. Child pornography collectors, and smart-phone and tablet users in general, commonly “sync” their devices with their personal computers or use their personal computers or external storage media to store photos and videos from their smartphones or tablet computers. Thus, photos, videos and other files from an individual’s smart-phone or tablet are also commonly found on their personal computers or laptops.

CONCLUSION AND REQUEST FOR SEALING ORDER

25. This investigation is ongoing, and disclosure of the search warrant, this affidavit, or this application and the attachments thereto will jeopardize its progress. For example, if the subjects of this investigation were notified that this investigation exists, they might destroy evidence, warn co-conspirators, or flee. Accordingly, I respectfully request the Court issue an order that the search warrant, this affidavit in support of the application for a search warrant, the application for this search warrant, and all attachments thereto, along with the order itself, be filed under seal until further order of this Court.

26. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the

locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the search and seizure of the items described in Attachment B.

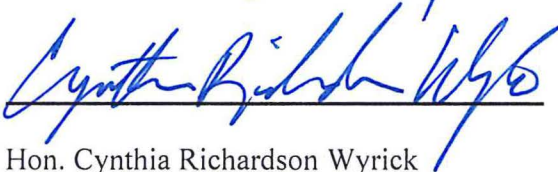


Special Agent Peter Evans

Homeland Security Investigations

Subscribed and sworn to before me by telephone

This 31st day of January, 2023



Hon. Cynthia Richardson Wyrick

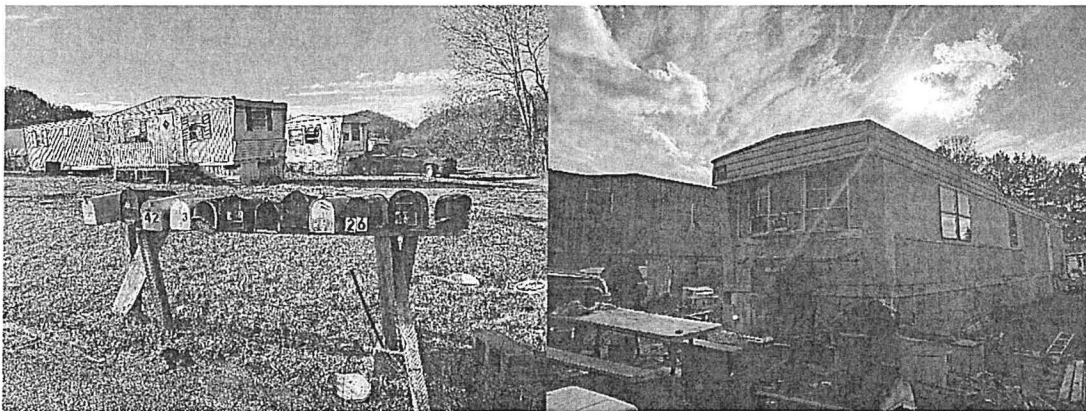
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

SUBJECT PREMISES:

656 Mountain View Road, Lot 27, Bluff City, TN 37618 (“**SUBJECT PREMISES**”) is a residential prefabricated mobile home (trailer), white and tan in color with the number 27 clearly visible on the front of the trailer. The number 27 is also visible on a mailbox located at the entrance with other mailboxes for the mobile homes on that street. A photograph is produced below. The premises to be searched includes the entirety of the residence, all rooms, attics, basements, closed and/or locked containers and safes, computers, and storage media found therein, and other places therein which are part of the **SUBJECT PREMISES** and the surrounding grounds, including storage areas, utility sheds, garages, mailboxes, trash containers, and out-buildings whether attached or detached that are not part of the common areas of the complex. The search shall also include vehicles under the dominion and control of Thomas LLOYD that are present at the residence during the execution of the search warrant. The search shall also include the person of Thomas LLOYD during the execution of the search warrant.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18 U.S.C. § 2252, as follows:

1. Data and information contained in smartphones, tablet computers, computers, laptops, computer media, external data storage devices, and digital media players and all such equipment containing such data and information, including any computer systems, smartphones, tablet computers, digital storage media (such as CD-ROMs, DVD-ROMs, thumb drives, or external hard drives), analog storage media (such as film, tapes or cassettes), and related peripherals (such as printers, monitors, keyboards, mice, scanners, players, projectors, and modems), commercial software applications, disk application programs, hardware and software operating manuals, video game consoles, cellular phones capable of accessing the Internet or storing computer files, still or video cameras, digital or analog photographs, digital or analog videos, undeveloped photographic film, slides, iPhones, Samsung Galaxy Phones, and other smartphones, iPods and other digital media storage and playback devices, passwords, power cords, data security devices and related documentation, related to or used to:
 - a. Visually depict minors engaged in sexually explicit conduct;
 - b. Contain information pertaining to a sexual interest in children or in child pornography;
 - c. Distribute, receive, or possess child pornography; or
 - d. Communicate with or about minors engaged in sexually explicit conduct;

e. Evidence related to the sexual exploitation of a child, such as any visually explicit images/videos, negatives, slides, books, magazines, videotapes, photographs, or other similar visual reproduction or depiction by computer (specifically including such images/videos as stored within computer storage devices as computer data files or on remote servers such as OneDrive, Google Drive, Google Photos, IDrive, Dropbox, Mega, iCloud, etc. using credentials or login information stored on the device or already known through the investigation) depicting any child known or reasonably believed to be under the age of 18 years of age engaged in sexual acts and/or poses, and believed to constitute child pornography.

2. Books, magazines, or other printed matter containing visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256, or describing such conduct;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Video recordings of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

5. Information, electronic records, or correspondence pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, including:

a. Information regarding Internet sites or peer-to-peer networks and participants in such sites or networks;

b. Envelopes, letters, and other correspondence including, but not limited to electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

c. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Records showing occupancy or ownership of the **SUBJECT PREMISES**, as more fully described in Attachment A, attached and incorporated herein by reference, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

7. Records or other items that indicate ownership or use of computer equipment found in the **SUBJECT PREMISES**, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes pertaining to such equipment.

8. Records, electronic or otherwise, or other items that relate to peer-to-peer software or networks, or to use of such software or networks by individuals who exhibit a sexual interest in children.

9. For any computer or electronic storage media, to include smartphones or tablet computers, described herein (and referred to herein as the **DEVICE**):

a. Evidence of who used, owned, or controlled the **DEVICE** at the time the things described in this warrant were created, edited, stored, saved, downloaded, uploaded, or deleted, such as logs, registry entries, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, electronically-stored photographs, and correspondence;

b. Evidence of software that would allow others to control the **DEVICE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. Evidence of the attachment to the DEVICE of other storage devices, disks, CD-ROMs, or similar containers for electronic evidence;
- d. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;
- e. Evidence of when and how the DEVICE was used;
- g. Passwords, encryption keys, and other access devices that may be necessary to access the DEVICE;
- h. Contextual information necessary to understand the evidence described in this attachment; and
- i. Any records, ledgers, correspondence or hand-written notes containing key-word search terms related to child pornography or references to websites related to child pornography.